

The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE

Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.

<http://www.us-cert.gov/tlp/>

DATE(S) ISSUED:

12/17/2020

SUBJECT:

A Vulnerability in Hewlett Packard Enterprise Systems Insight Management Could Allow for Remote Code Execution

OVERVIEW:

A vulnerability has been discovered in Hewlett Packard Enterprise (HPE) Systems Insight Management (SIM) which could allow for remote code execution. HPE SIM is a management and remote support automation solution for multiple HPE servers, storage, and networking products. Successful exploitation of this vulnerability could allow for remote code execution. Depending on the privileges associated with the user an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

THREAT INTELLIGENCE:

There are currently no reports of this vulnerability being exploited in the wild.

SYSTEMS AFFECTED:

- HPE Systems Insight Manager versions 7.6.X

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:

A vulnerability has been discovered in Hewlett Packard Enterprise (HPE) Systems Insight Management (SIM) which could allow for remote code execution. This vulnerability results from the lack of proper validation of user-supplied data that can result in the deserialization of untrusted data making it possible for an attacker to leverage it to execute code on servers

running vulnerable software. Successful exploitation of this vulnerability could allow for remote code execution. Depending on the privileges associated with the user, an attacker could then install programs; view; change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate updates provided by Hewlett Packard to vulnerable systems, immediately after appropriate testing when available.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services

REFERENCES:

Hewlett Packard:

https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbgn04068en_us

CVE:

<https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2020-7200>

Bleeping Computer:

<https://www.bleepingcomputer.com/news/security/hpe-discloses-critical-zero-day-in-server-management-software/>

TLP: WHITE

Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.

<http://www.us-cert.gov/tlp/>